Docket # 4283
USSN: 10/617,309

AD

(12) UK Patent Application (19) GB (11) 2 119 548 A

(21) Application No 8207775
(22) Date of filing 17 Mar 1982
(43) Application published
16 Nov 1983
(51) INT CL³
E05B 47/00 B60R 25/00
(52) Domestic classification
G4H 13D 14A 14B 14D
14G 1A 60 RBE RCE TG
U1S 1693 1772 1792
1820 G4H
(56) Documents cited
GB A 2051442
GB A 2046827
GB A 2041599
GB 1595797
GB 1595796
GB 1492491
WO A 8103002
(58) Field of search
G4H
(71) Applicants
John Robert Carter,
1 Gairloch Avenue,
Bletchley,
Milton Keynes,
MK2 3DH,
Pasquale Straccia,
3 Colchester Way,
Bedford,
Bedfordshire
(72) Inventors
John Robert Carter,
Pasquale Straccia
(74) Agent and/or address for service
Marks and Clerk,
57—60 Lincolns Inn
Fields,
London,
WC2A 3LS

(54) Locking systems

(57) A locking system comprises a transmitter 1 which transmits a predetermined code by non-contact means, such as infrared waves. A receiver 2 receives the codes and provides an access-permitting signal, for instance to a vehicle door lock, when a received code is identified as the predetermined code.

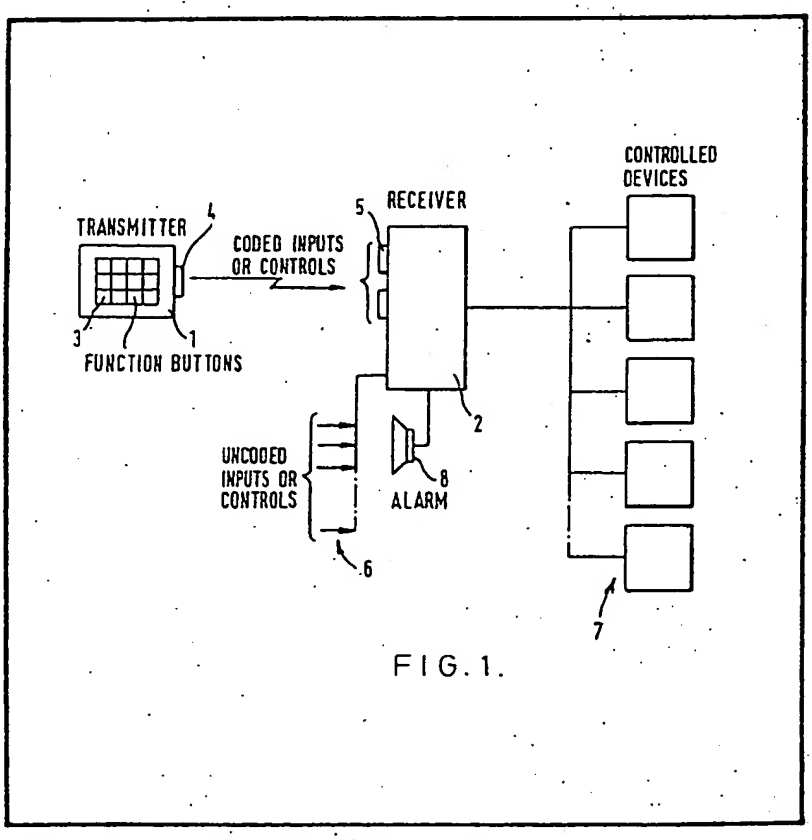


FIG.1.

GB 2 119 548 A

The drawings originally filed were informal and the print here reproduced is taken from a later filed formal copy.

2119548

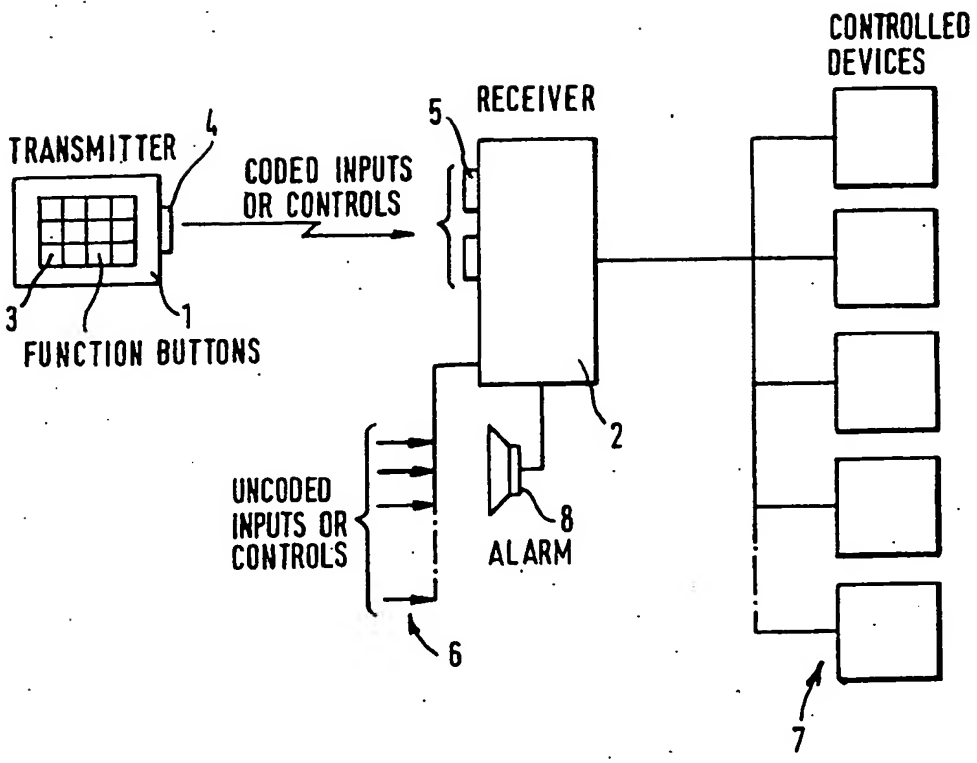


FIG.1.

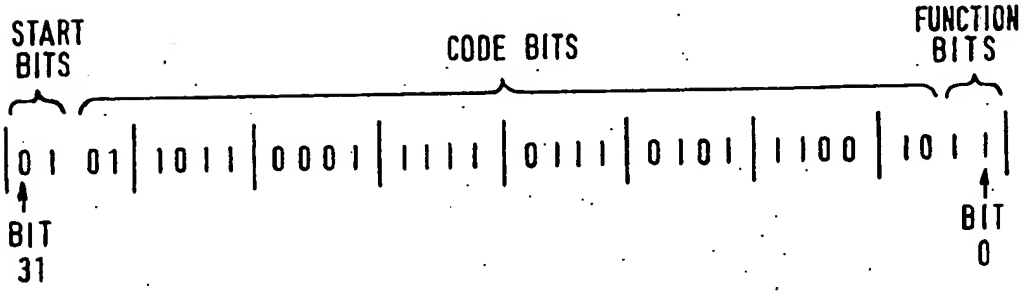


FIG.2.

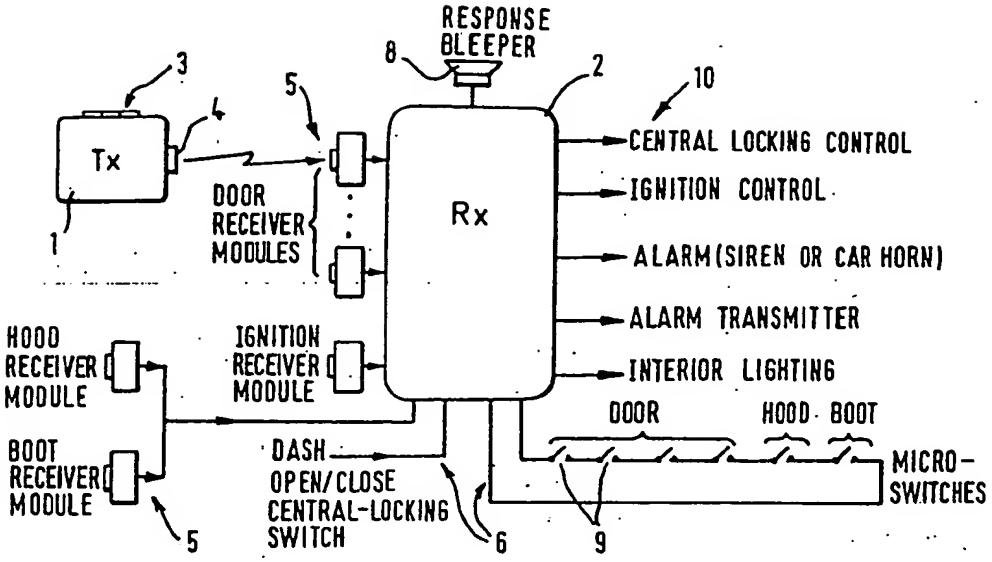

RESPONSE BLEEPER
8
2
10
3
4
5
Tx
1
DOOR RECEIVER MODULES
Rx
CENTRAL LOCKING CONTROL
IGNITION CONTROL
ALARM (SIREN OR CAR HORN)
ALARM TRANSMITTER
INTERIOR LIGHTING
HOOD RECEIVER MODULE
IGNITION RECEIVER MODULE
DOOR
HOOD
BOOT
BOOT RECEIVER MODULE
DASH OPEN/CLOSE CENTRAL-LOCKING SWITCH
MICRO-SWITCHES
5
6
9

FIG. 3.

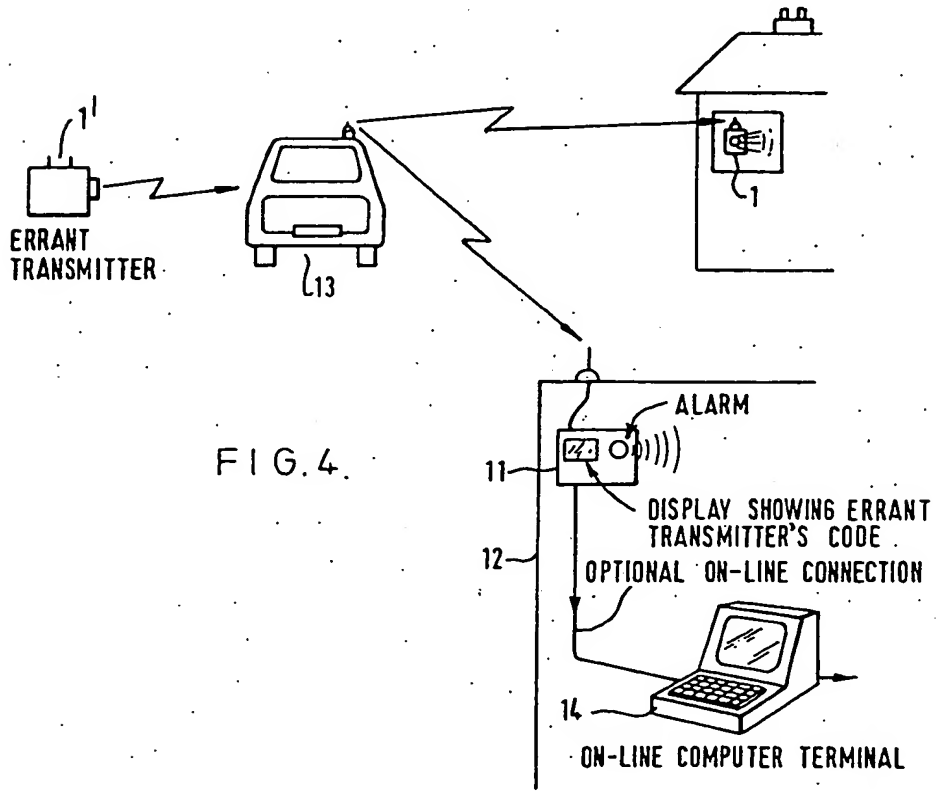
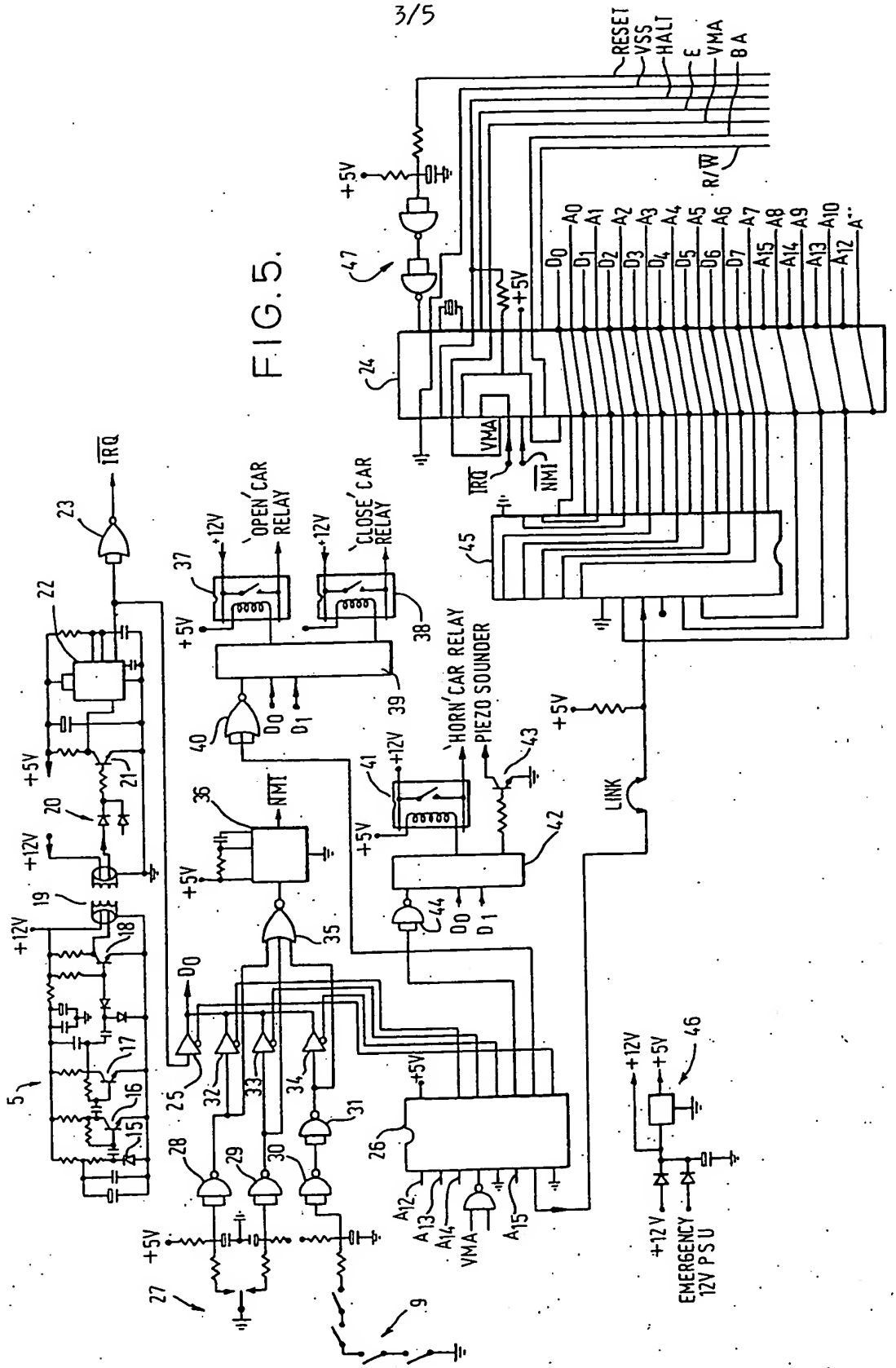

1'
ERRANT TRANSMITTER
13
1
ALARM
11
DISPLAY SHOWING ERRANT TRANSMITTER'S CODE
12
OPTIONAL ON-LINE CONNECTION
14
ON-LINE COMPUTER TERMINAL

FIG. 4.

FIG. 5.


RESET
VSS
HALT
E
VMA
BA
R/W
A0
A1
A2
A3
A4
A5
A6
A7
A8
A9
A10
A11
A12
A13
A14
A15
D0
D1
D2
D3
D4
D5
D6
D7
+5V
+12V
IRQ
NMI
VMA
OPEN CAR RELAY
CLOSE CAR RELAY
HORN CAR RELAY
PIEZO SOUNDER
LINK
EMERGENCY 12V PSU

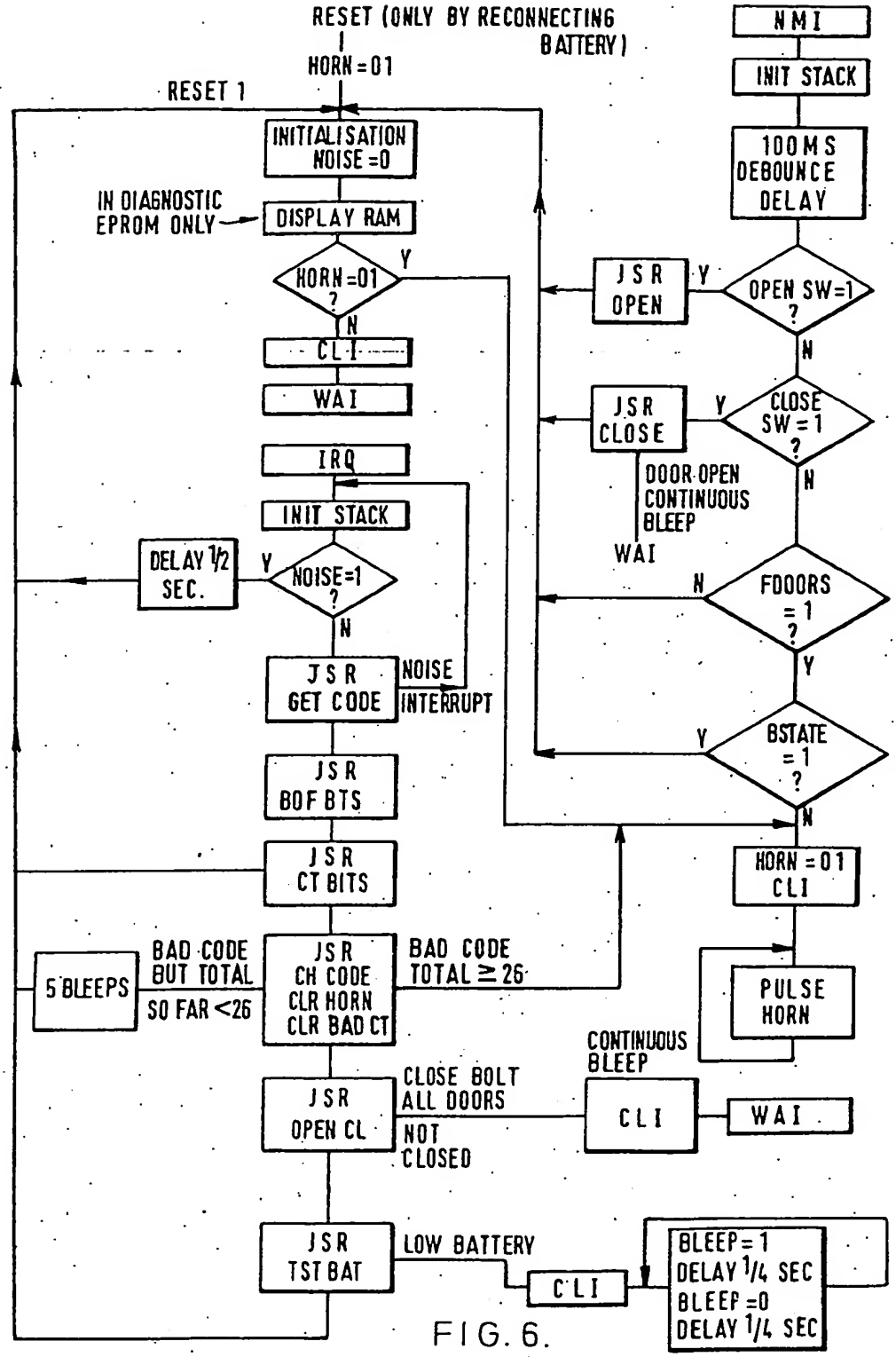

RESET (ONLY BY RECONNECTING BATTERY)
HORN=01
RESET 1
INITIALISATION NOISE=0
IN DIAGNOSTIC EPROM ONLY
DISPLAY RAM
HORN=01 ?
Y
N
CLI
WAI
IRQ
INIT STACK
DELAY 1/2 SEC.
Y
NOISE=1 ?
N
JSR GET CODE
NOISE INTERRUPT
JSR BOF BTS
JSR CT BITS
5 BLEEPS
BAD CODE BUT TOTAL SO FAR <26
JSR CH CODE CLR HORN CLR BAD CT
BAD CODE TOTAL ≥ 26
JSR OPEN CL
CLOSE BOLT ALL DOORS
NOT CLOSED
JSR TST BAT
LOW BATTERY
CLI
BLEEP=1
DELAY 1/4 SEC
BLEEP=0
DELAY 1/4 SEC
NMI
INIT STACK
100 MS DEBOUNCE DELAY
OPEN SW=1 ?
Y
JSR OPEN
CLOSE SW=1 ?
JSR CLOSE
DOOR OPEN CONTINUOUS BLEEP
WAI
FDOORS =1 ?
BSTATE =1 ?
HORN=01
CLI
PULSE HORN
CONTINUOUS BLEEP
CLI
WAI

FIG. 6.

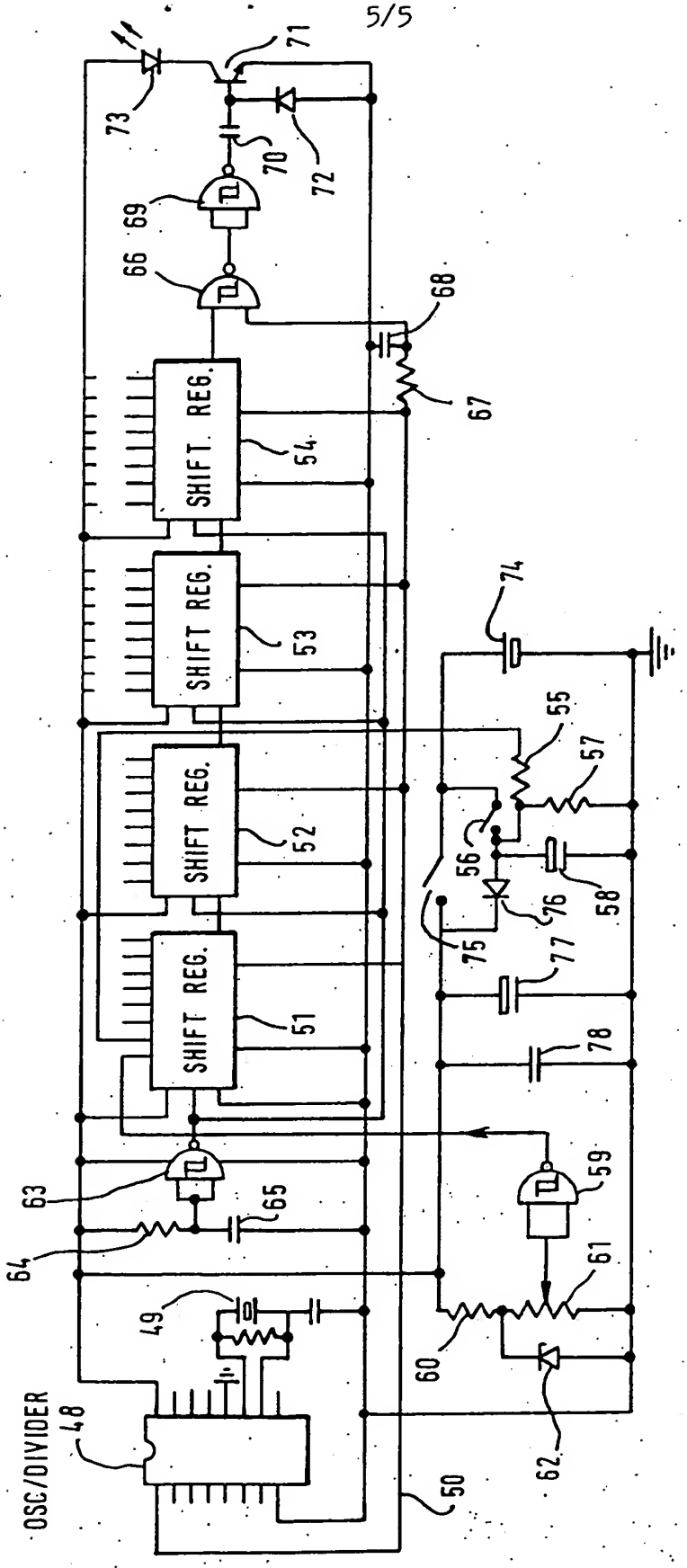

SHIFT. REG.
SHIFT REG.
SHIFT REG.
SHIFT REG.
OSC/DIVIDER
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78

FIG. 7.

SPECIFICATION

Improvements in or relating to locking systems

The present invention relates to locking systems. Such a system may be used to control access to a vehicle and may replace many of the mechanical parts of vehicle locks. Such systems, such as rooms, buildings, and safes. Further, such systems may be used to control access to further systems, such as data processing systems and electrical and electronic equipment in general.

According to the invention, there is provided a locking system comprising a transmitter arranged to transmit a predetermined code by non-contact means, and a receiver arranged to receive codes by non-contact means and to provide an access-permitting signal when a received code is identified as the predetermined code.

The non-contact means may comprise electromagnetic radiation, for instance in the infra-red region of the electromagnetic spectrum, or electromagnetic induction. Alternatively, the non-contact means may comprise acoustic waves of ultrasonic frequence. In general, the non-contact means may be any information carrier which does not require physical contact or connection between the receiver and the transmitter.

The predetermined code may be in the form of binary code representing a predetermined number and possibly including additional bits, for instance to transfer information or control signals to apparatus with which the receiver may be associated. When the locking system is used to control access to an enclosed space, such additional bits may be used to control whether the access-permitting signal actuates locking or unlocking of access means, such as a door. Preferably, the non-contact means comprises a carrier wave which is modulated by the binary code so as to comprise burst of carrier wave representing a first type of digit and gaps representing a second type of digit, the binary code comprising a predetermined minimum number, greater than zero, of digits of the first type, the transmitter being arranged to transmit the digits in predetermined portions of consecutive time windows, and the receiver being arranged to prevent the production of the access-permitting signal upon detecting signals outside the said portions. This provides the system with very good immunity to noise or spurious signals.

Preferably, the receiver is arranged to produce an alarm signal upon receipt of a number of codes, greater than a predefined number (such as 25), not identified as the predetermined code. The system is thus provided with a high level of security against unauthorised attempts to break the code and gain access. For instance, where a binary code having 28 bits defining the predetermined code is used, and the code has at least ten non-zero bits to provide noise immunity, the chances of finding the correct code by 25 random attempts is approximately one in ten million.

Preferably, the receiver includes transmitting means for transmitting a signal indicative of tampering upon receipt of more than the predefined number of unidentified codes. The transmitting means may be arranged to send a predefined code, preferably different from the predetermined code, to permit identification of the system which is being subjected to tampering. The transmitter may include receiving means for receiving the signal indicative of tampering, and may be arranged to respond only to the predefined code.

According to another aspect of the invention, there is provided a method of validating a signal, comprising forming the signal in a plurality of consecutive time windows such that the signal occupies predetermined portions of the time windows and such that the signal in at least one of the predetermined portions has a non-zero level, and monitoring parts of the time windows different from the predetermined portions for the presence of signal levels which are above a predetermined value and which are thus indicative of an invalid signal.

The invention will be further described by way of example, with reference to the accompanying, in which:

Figure 1 is a block diagram of a locking system constituting a first embodiment of the invention;

Figure 2 illustrates the format of a predetermined code used in the system of Figure 1;

Figure 3 is a block diagram of a locking system, for use in a motor vehicle, constituting a second embodiment of the invention;

Figure 4 illustrates a mode of operation of the system of Figure 3;

Figure 5 is a circuit diagram of a receiver of the system of Figure 3;

Figure 6 is a flow diagram illustrating operation of the receiver of Figure 5; and

Figure 7 is a circuit diagram of a transmitter of the system of Figure 3.

The locking system shown in Figure 1 comprises a transmitter 1 and a receiver 2. The transmitter 1 has a keyboard 3 for controlling operation thereof and an output 4 which includes an infra-red light emitting diode.

The receiver 2 has infra-red detectors 5 for receiving infra-red signals transmitted by the transmitter 1. The receiver further has a plurality of inputs 6 for supplying local input and control signals to the receiver. The receiver is arranged to control access to an enclosed space or to electrical or electronic equipment, and control access thereto. For this purpose, a plurality of controlled devices 7 are provided. Further, an audible alarm 8 is connected to the receiver 2.

The transmitter 1 is arranged to modulate the infra-red signals produced by the output 4 with a predetermined code, for instance in the form of a binary code. The receiver 2 is arranged to receive infra-red signals by means of the sensors 5 and to detect the code which such signals carry. The detected code is compared with a predetermined

code in the receiver and, if the two codes coincide, an output signal is supplied by the receiver to the controlled devices 7. The controlled devices may, for instance, be electro-mechanical locks which are unlocked upon receipt by the receiver 2 of the correct predetermined code. Thus, the transmitter and receiver can replace the conventional key and lock arrangement provided for controlling access through doors or the like.

If the receiver 2 detects an incorrect code for greater than a predetermined of times, then it will prevent the control devices 7 from being actuated and sounds an alarm by means of the audible alarm 8. In a preferred embodiment, the alarm may only be disabled when the receiver receives the correct predetermined code from its corresponding transmitter.

As mentioned above, the transmitter 1 pressurably supplies a predetermined code in the form of binary digits which modulate the infra-red carrier. The binary code is thus transmitted in series and Figure 2 illustrates a possible type of code which may be used in the system of Figure 1. The code always begins with two start bits which always have the values 0 and 1 as shown. This alerts the receiver to the presence of the code and allows timing of the receiver to be synchronised. The following 28 bits define a code which is unique or essentially unique to the combination of the transmitter and receiver, so that each such combination has a different code. The use of 28 bits for this code provides a high degree of security as there a relatively large number of possible codes which could be employed. The final two bits serve to control the functioning of the receiver 2 and the associated controlled devices 7. For instance, the first of these bits may be zero when the receiver is to be controlled so as to actuate the controlled devices 7 and 1 when the receiver is to deactivate the controlled devices. Thus, zero would correspond to opening or unlocking a door and 1 would correspond to closing or locking the door. The second function bit may be zero to indicate that a battery which powers the transmitter 1 is nearing the end of its useful life. This bit may then be used to trigger an audible warning at the receiver 2 so that the battery of the transmitter can be replaced in good time.

Figure 3 illustrates a locking system similar to that of Figure 1 but specifically intended for use in controlling access to a vehicle. The parts in Figure 3 which correspond to parts in Figure 1 are referred to by like reference numerals. The transmitter 1 is provided with a key-board 3 having only two keys which control locking and unlocking of the vehicle or car doors. The sensors 5 include sensors arranged to respond to infra-red signals aimed at the doors of the car, sensors arranged to receive infra-red signals aimed at the boot and bonnet of the car, and a sensor arranged to receive signals for activating the ignition mounted on the dash-board of the car. The audible alarm may be located in or behind the dash-board of the car but should be audible from outside the car.

The inputs 6 to the receiver 2 comprise a first input responsive to a central locking/unlocking switch provided in the car for manual actuation of the door locks and boot and bonnet locks. A second input comprises a series connection of micro-switches 9 which normally provide a closed circuit but which are opened when any of the doors, the boot, or the bonnet is open or not properly closed.

The receiver 2 has a plurality of outputs 10 which control central locking of the doors, boot, and bonnet, the ignition system, an alarm such as a siren or the car horn, an alarm transmitter, and the interior light of the car.

Operation of the locking system shown in Figure 3 is as follows, starting with an unlocking operation assuming that a driver wishes to gain access to the car, all of whose doors are closed and locked. The owner or driver of the car has, in place of the conventional door key, transmitter 1 which contained the correct predetermined code for operating the receiver 2. The driver thus aims the transmitter 1 at one of the door sensors 5 and presses the one of the buttons of the keyboard 3 for opening or unlocking the door locks. The receiver 2 receives the predetermined code, checks this against its stored predetermined code and as a result of the coincidence therebetween unlocks the door locks.

However, if the incorrect transmitter is used to attempt to open the car, then the code received by the receiver 2 is not identified as the predetermined code and the door locks remain locked. The receiver 2 is programmed so as to allow a relatively small number of attempts, for instance 25, to be made to open the door, after which an alarm signal is provided, for instance by means of the vehicle horn, the door locks remaining locked. A signal is supplied to the ignition control, but rendering the engine of the vehicle inoperative. Further, the control signal is set to the alarm transmitter (not shown) which sends via a radio frequency carrier a signal to the owner and possibly also in the local police station as indicated in Fig. 4. Figure 4 illustrates the incorrect transmitter at 1′ and shows an apparatus 11 located at a local police station 12. The alarm transmitter send a code, different from the predetermined code of the receiver, which is unique to the transmitter 1. The transmitter 1 includes a receiving means which receives this code and emits an audible alarm to warn the driver that an attempt is being made to break into the vehicle 13. The signal transmitted by the alarm transmitter may also include details of the code which is being used by the incorrect transmitter 1′ and this information may be used by the police to assist in identifying the person attempting to break into the car. For instance, the apparatus 11 may display this code and may supply it to an on-line computer terminal 14 which has access to a data base, so as to attempt to identify the person the incorrect transmitter 1′.

The only way in which the signal transmitted by the alarm transmitter can be disabled is by using the correct transmitter 1 to supply its predetermined code to the receiver 2 in the car. Thus, the locking system provides a high degree of security as regards gaining access to the car.

The receiver 2 contains a microprocessor for controlling all operations of the locking system. The microprocessor is controlled by a programme for instance stored in a programmable read-only memory. When the correct predetermined code is received by the receiver 2, a single "bleep" which is audible outside the car is produced by means of the audible alarm 8. Thus, pressing of the "open" key of the keyboard 3 causes the locks of the car to be unlocked and the bleep indicates this to the driver.

Each time an incorrect code is received, the device 8 produces five bleeps. This can be caused, not only by the use of an incorrect code, but also by poor aiming of the transmitter, thus indicating that the driver should approach closer to the car, aim the transmitter more accurately and try again.

Once the owner is inside the car, together with any passengers, the doors may all be locked by means of a central locking switch on the dashboard. Such locking switches are already present in many types of cars, but other types of cars may be adapted appropriately by providing a central locking system. If all the doors, the bonnet and the boot are closed so that all the microswitches 9 are closed, two bleeps are produced by the device 8 and all the locks are locked. However, if any microswitch 9 is open, no bleep is produced and, optionally, the ignition system is disabled so that the car cannot be driven until all doors and the like are closed. The ignition system is enabled by again actuating the transmitter 1 and directing it towards the ignition sensor 5, after which the engine may be started and the car may be driven.

When the driver and where appropriate, passengers wish to leave the car, the driver uses the central locking switch to unlock all the doors and the occupants leave the car and close the doors. The driver may then press the "close" button of the keyboard 3 while directing the transmitter 1 towards the appropriate door sensor 5. Again, if any of the doors or the boot or the bonnet is not completely closed, the device 8 produces a continuous bleep so that the offending door or the like can be closed and the appropriate button on the transmitter pressed again. Assuming that all doors and the like are not closed, two bleeps are sounded by the device 8 and all the locks are locked. If an attempt is made by an unauthorized person to gain entry to the vehicle without using any form of transmitter 1, then one of the microswitches 9 will be opened so that the receiver produces an alarm and disables the ignition. The microprocessor of the receiver 2 is further programmed to cause an alarm whenever disconnection and reconnection of the car battery takes place, so that the system cannot be immobilised by temporarily disconnecting the battery. Such an alarm can be immobilised only by operating the correct transmitter 1, for instance should it be necessary to remove or replace the battery.

In order to prevent the receiver 2 responding to noise or spurious infra-red signals for instance caused by the headlight beams of passing cars, the microprocessor contained within the receiver 2 is programmed so that the receiver is sensitive only to codes having the correct format. For this purpose, the transmitter 1 is arranged to supply each digit of the code during a predetermined initial portion of a corresponding time window, which may for instance be 4.096 m/seconds. Between each digit, there is a period of 2.9 m/seconds in each time window when no information is transmitted. The microprocessor of the receiver 2 continues monitoring during this listening period and, if any none-zero signals are detected, then the input signal is assumed to be noise and is disregarded by the receiver 2. Thus, the system has a very high degree of immunity to noise or other spurious signals.

In order to make this noise suppression system viable, it is necessary to ensure that the predetermined code contains a number of binary digit ones. For instance in a preferred embodiment, it is a requirement that every predetermined code should have a minimum of ten ones. In the case of a system employing a predetermined code of 28 nits, in which the system permits 25 attempts to supply the correct predetermined code before raising an alarm, this provides only one chance in ten million of an authorised person being able to find the correct code.

Although the system shown in Figure 3 is specifically intended for use with a vehicle a simliar type of system may be used to control access to data processing equipment. For instance, the transmitter 1 may be provided with a larger keyboard for instance a ten digit numeric keyboard allowing numerical data to be sent to equipment to be controlled. Alternatively the keyboard may comprise a miniature ASCII keyboard, for instance of the type used with pocket computers, to allow messages to be typed into devices, such as the front door of a company building provided with a receiver connected into an office communication system or a cash point terminal.

The locking system of Figure 3 may be used to replace completely the mechanical system using a conventional key in motor cars and the like. Further, the system gives a much higher degree of security to a vehicle than is possible with conventional mechanical locking arrangements. Further the system may include any combination of the following features:

Use of a transmitter 1 without an ON-OFF switch with the buttons of the keyboard 3 serving to activate the transmitter by connection of the battery, thus giving a life span to the battery of, for instance, ten years;

the presence of a Schmitt Trigger in the transmitter 1 for detecting when the battery condition is low and to supply a signal to the receiver to warn the user;

arrangement of the microswitches 9 to activate a non-maskable interrupt of the microprocessor in the receiver 3 to indicate an attempted forced entry;

Correct operation of the system in direct sunlight by using as each of the sensors 5 an infra-red receiving diode which is heavily reversed biased.

Such a system thus has substantial advantages with respect to the conventional mechanical locking system used, for instance, in vehicles. For instance, problems caused by the conventional exposed mechanical locking mechanisms, such as freezing up, are completely avoided as the system operates electronically and need have no exposed parts. Such a system is also easier to operate by the aged and disabled as the locking function can be performed remotely. Further, when such a system is used to control access, for instance, to a safe or building, each employee may be given a transmitter having a different predetermined code and the receiver may be made sensitive to these codes. Thus, it is possible at any time to establish who is in the building. Further, the system may be used to perform a "clocking-in" function for employees.

Figure 5 is a circuit diagram of the receiver shown in Figure 3. each of the infra-red sensors 5 comprises an infra-red sensitive diode 15 connected to a pulse amplifier comprising transisters 16, 17 and 18. The sensors 5 are disposed adjacent the doors, boot, and bonnet of the vehicle and are connected via respective screened leads 19 to respective diodes 20. The diodes 20 and the following amplifier including transistor 21 form an OR gate with the output of the amplifier being connected to an integrated circuit 22 which functions as a monostable multivibrator having a pulse period of approximately 0.47m/seconds. The output signal from the monostable multivibrator are supplied via a gate 23 connected as a buffer to an input $\overline{IRQ}$ of an integrated circuit microprocessor 24 which commences decoding of the received code as soon as a start pulse of logic level is received. The output signals of the monostable multivibrator are also supplied to the least significant line of a data buzz via a tri-state buffer 25. All addressed decoding functions for input and output devices is provided by means of an address decoder integrated circuit 26.

Whenever a logic level 1 is supplied to the input $\overline{IRQ}$ or the microprocessor 24 at an interrupt signal during a listening period as described hereinabove, the microprocessor sets a flag NOISE in its own random access memory. A softwear timing loop then provides a delay of half a second, after which the program resets. This operation is illustrated in the flow diagram shown in Fig. 6 of the drawings, further description of which will be given hereinafter.

The door, bonnet and boot microswitches 9 and a central locking switch 27 are connected, via respective resistor-capacitor networks for suppressing contact balance effects, to the inputs of respective gates 28, 29 and 20. The outputs of these gates are connected via inverters 31 to 34, together with the output of the gate 25 to the least significant line D_0 of the data bus whereas the outputs of the gates 28 and 29 and of the inverter 31 are connected via an OR gate 35 to the input of a second monostable multivibrator 36. The output of the monostable multivibrator 36 is connected to an input NMI of the microprocessor 24 to supply non-maskable interrupt signals thereto.

It is assumed that the vehicle incorporating the receiver shown in Figure 5 already has a central locking system including "open" and "closed" relays for operating the solenoid locks of the car doors, the boot and the bonnet. The receiver includes first and second relays 37 and 38 having contacts for operating the "open" and "closed" relays respectively of the car. The windings of the relays 37 and 38 are connected to respective outputs of a latch 39 which receives enable signals via an inverter 40 from the address decoder 26. A third relay 41 is provided for controlling the car horn relay and has a winding connected to an output of a latch 42. The device 8 in Figure 3 is constituted by a piezo electric sounder connected via a buffer transistor 43 to another output of the latch 42. Enable signals for the latch 42 are supplied via an inverter 44 from an output of the address decoder 26.

The receiver shown in Figure 5 has various other parts such as a read-only memory 45, a power supply 46, and a switch-on reset circuit 47, with the microprocessor 24 and the read-only memory 45 being connected together by address and data buses.

Figure 6 is a flow diagram illustrating operation of the microprocessor 24 in the receiver of Figure 5. Upon connecting the battery to the receiver, the circuit is reset and this causes the horn to sound, thus preventing a potential thief from disabling the alarm by temporarily disconnecting the battery. The only way in which the horn may then be stopped is by the receiver decoding its predetermined code as stored in the read-only memory 45. Alternatively, the predetermined code for the receiver, and also for the transmitter, may be changeable, for instance by means of 7 hex switches so that the predetermined code may be changed from time to time.

Upon receipt of a start pulse, a routine $\overline{IRQ}$ is started and decodes the input data stream to supply the result into four bites of the random access memory of the microprocesor. The number of logic level 1's is counted by the subroutine CTBITS and, if less than ten, a reset occurs and the input is assumed to be noise.

The received and decoded input code is compared with the stored predetermined code and in the absence of a match, a counter BADCT is incremented. If this happens more than, for

instance, 25 times, then the alarm is raised. This alarm can only be disabled by receipt of the correct code. Each time an incorrect code is received, five bleeps are produced by the piezo electric sounder.

Upon receipt of the correct predetermined code, a subroutine OPENCL decodes the open/close function bit of the received code. If this function bit indicates "close" and not all of the doors, boot and bonnet are fully closed then a continuous bleep results which can be stopped only by closing the door and resending the "close" code.

A subroutine TSTBAT then inspects the last function bit and, if this is a logic level zero, causes a pulsing bleep to be produced by the sounder until the driver operates the internal central locking switch. This provides a reminder to the driver to replace the battery in the transmitter. However, with the transmitter circuit described hereinafter, this is unlikely to occur within the life of a car because of the low coned consumption of the transmitter.

Operation of the central locking switch causes a non-maskable interrupt NMI, according to which the microprocessor inspects the state of the central working switch to ascertain whether an open or closed command has been made. If neither command has been made, then the microprocessor inspects the microswitches, which can also signal a non-maskable interrupt N,O. When an open command is received, the door locks are opened. When a close command is received and a door is still open, a continuous bleep is made by the sounder indicating danger to occupants of the car if it were to be driven. Otherwise, the doors are locked. If the interrupt signal comes from a door microswitch and BSTATE=1 (i.e. the last command was to lock the door) then this represents a forced door opening and an alarm is sounded. The only way in which the alarm can then be stopped is by receipt of the correct predetermined code.

Figure 7 is a circuit diagram of the transmitter 1 of Figure 3. The transmitter comprises an oscillator/divider integrated circuit 48 to which is connected a 1 MHz quartz crystal 49 for controlling the frequency of operation. The divider of the integrated circuit 48 divides the 1 MHz output of the oscillator by numerals 4096 to provide output pulses on a line 50 having a period of 4.096 m/seconds.

The transmitter further comprises four 8 bit parallel input serial output shift registers 51 to 54, each having a clock input connected to the line 50. The cascade connected shift registers thus have a combined capacity of 32 bits. Starting from the right hand end of the cascade connected shift registers, the first 30 parallel inputs are connected to logic levels defining the start bits and the predetermined code. The 31st bit of this shift register arrangement is connected via a resistor 55 to the "close" key switch 56 and to one end of a parallel arrangement comprising a resistor 57 and a capacitor 58. The 32nd bit of the shift register arrangement is connected to the output of a Schmidt trigger gate 59 connected as an inverter. The input of the gate 59 is connected to a potential divider comprising a resistor 60 and a variable resistor 61, across which is connected a zener diode 62.

The load inputs of the shift registers 51 to 54 are connected to the output of a gate 63 connected as an inverter. The input of the gate 63 is connected to a switch-on delay circuit comprising a resistor 64 and a capacitor 65.

The output of the shift register 54 is connected to one input of a Schmitt trigger AND gate 66, whose other input if connected via a delay circuit comprising a resistor 67 and a capacitor 68 to the line 50 so as to receive the output pulses from the integrated circuit 48. The output of the gate 66 is connected via another gate 69 wired as an inverter and via a capacitor 70 to the base of a transistor 71, which has a diode 72 connected in anti-parallel with the base-emitter junction to prevent transmission of a spurious "1" when the "open" key switch is actuated. The collector of the transistor 71 is connected to an infra-red light emitting diode 73.

A mercury cell battery 74 supplies power to the transmitter via the key switch 56 or the "open" key switch 75, a diode 76 being provided to isolate the capacitor 58 and the resistor 57 from the power supply line when the key switch 75 is actuated. Capacitors 77 and 78 perform a debouncing function for the key switches 56 and 75.

Until one of the key switches 56 and 75 is actuated, the battery 74 is disconnected from the circuit of the transmitter to provide zero quiescent power consumption for the transmitter. The gate 59 and associated circuitry supply a logic level zero or one signal to the last input of the shift register 51 according to whether the battery condition is too low or adequate. When the key switch 75 is closed, the resistors 55 and 57 supply a logic level zero signal to the penultimate input of the shift register whereas, when the key switch 56 is actuated, a logic level 1 is supplied to this input. Upon actuation of either key switch, the battery is connected to the power supply lines of the transmitter and the delay circuit comprising the resistor 64 and the capacitor 65 supplies, via the gate 63, a load signal for a predetermined period, such as 90 m/seconds. Thus, the logic levels present at the parallel inputs of the shift registers 51 to 54 are loaded in the registers. The shift registers are then clocked by the output pulses from the integrated circuit 48 and the output pulses of the shift register 54 are combined in the NAND gate 66 with the delayed output pulses. The output pulses from the gate 66 control transmission by the diode 73 of infra-red pulses.

The transmitter of Figure 7 is constructed entirely from CMOS integrated circuits so as to have a very low battery consumption, for instance of 2 m/amps, when one of the key switches 56 and 75 is actuated. Further, the output pulses

corresponding to logic level 1's at the output of the gate 66 are very narrow, thus also aiding the relatively low current consumption of the circuit. The debouncing capacitors 77 and 78 has sufficient capacity to ensure that transmission of the complete code stored in the shift registers occurs even for only a momentary closure of either of the key switches 56 and 75.

Claims (Filed on 27/5/82)

1. A locking system comprising a transmitter arranged to transmit a predetermined code by non-contact means, and a receiver arranged to receive codes by non-contact means, and a receiver arranged to receive codes by non-contact means and to provide an access-permitting signal when a received code is identified as the predetermined code.

2. A system as claimed in claim 1, in which non-contact means comprises electromagnetic radiation, for instance in the infra-red region of the electromagnetic spectrum, or electromagnetic induction.

3. A system as claimed in claim 1, in which the non-contact means comprises acoustic waves of ultrasonic frequence.

4. A system as claimed in any one of the preceding claims, in which the predetermined code is in the form of binary code representing a predetermined number.

5. A system as claimed in claim 4, in which the non-contact means comprises a carrier wave which is modulated by the binary code so as to comprise bursts of carrier wave representing a first type of digit and gaps representing a second type of digit, the binary code comprising a predetermined minimum number, greater than zero, of digits of the first type, the transmitter being arranged to transmit the digits in predetermined portions of consecutive time windows, and the receiver being arranged to prevent the production of the access-permitting signal upon detecting signals outside the said portions.

6. A system as claimed in any one of the preceding claims, in which the receiver is arranged to produce an alarm signal upon receipt of a number of codes, greater than a predefined number, not identified as the predetermined code.

7. A system as claimed in claim 6, in which the receiver includes transmitting means for transmitting a signal indicative of tampering upon receipt of more than the predefined number of unidentified codes.

8. A system as claimed in claim 7, in which the transmitting means is arranged to send a predefined code, preferably different from the predetermined code, to permit identification of the system which is being subjected to tampering.

9. A system as claimed in claim 8, in which the transmitter includes receiving means for receiving the signal indicative of tampering, and is arranged to respond only to the predefined code.

10. A method of validating a signal, comprising forming the signal in a plurality of consecutive time windows such that the signal occupies predetermined portions of the time windows and such that the signal in at least one of the predetermined portions has a non-zero level, and monitoring parts of the time windows different from the predetermined portions for the presence of signal levels which are above a predetermined value and which are thus indicative of an invalid signal.

Printed for Her Majesty's Stationery Office by the Courier Press, Leamington Spa, 1983. Published by the Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.